Бублик фб62

1. Побічні електромагнітні випромінювання та наведення (ПЕМВН). Суть програм створення засобів, захищених від витоку інформації за рахунок ПЕМВН;

**Короткий опис можливого витоку інформації каналами ПЕМВН**

3.1 Можливі канали витоку інформації утворюються:

- низькочастотними електромагнітними полями, які виникають під час роботи ТЗПІ та ДТЗС;

- під час впливу на ТЗПІ та ДТЗС електричних, магнітних та акустичних полів;

- під час виникнення паразитної високочастотної (ВЧ) генерації;

- під час проходження інформативних (небезпечних) сигналів у колі електроживлення;

- під час взаємного впливу кіл;

- під час проходження інформативних (небезпечних) сигналів у колі заземлення;

- під час паразитної модуляції високочастотного сигналу;

- внаслідок хибних комутацій і несанкціонованих дій.

3.2 Під час пересилання інформації з обмеженим доступом в елементах схем, конструкцій, підвідних і з`єднувальних проводах технічних засобів протікають струми інформативних (небезпечних) сигналів. Електромагнітні поля, що виникають при цьому, можуть впливати на випадкові антени. Сигнали, прийняті випадковими антенами, можуть призвести до утворення каналів витоку інформації.

Джерелами виникнення електромагнітних полів у ТЗПІ та ДТЗС можуть бути неекрановані проводи, розімкнуті контури, елементи контрольно-вимірювальних приладів, контрольні гнізда на підсилювальних блоках і пультах, неекрановані кінцеві пристрої, підсилювачі потужності та лінійні підсилювачі, трансформатори, дроселі, з`єднувальні проводи з великими струмами, роз`єми, гребінки, гучномовці, кабельні лінії.

3.3 Інформативні (небезпечні) сигнали можуть виникати на елементах технічних засобів, чутливих до впливу:

- електричного поля (неекрановані проводи та елементи технічних засобів);

- магнітного поля (мікрофони, гучномовці, головні телефони, трансформатори, котушки індуктивності, дроселі, електромагнітні реле);

- акустичного поля (мікрофони, гучномовці, головні телефони, трансформатори, котушки індуктивності, дроселі, електромагнітні реле).

За наявності в технічних засобах елементів, здатних перетворювати ці поля в електричні сигнали, можливий витік інформації незахищеними колами абонентських ліній зв`язку, електроживлення, заземлення, керування, сигналізації.

3.4 Паразитна високочастотна генерація (ПВЧГ) у ТЗПІ та ДТЗС виникає внаслідок самозбудження підсилювальних пристроїв (активна ПВЧГ) або внаслідок відбиття сигналів від кінців ліній зв`язку між підсилювачами під час перехідних процесів (пасивна ПВЧГ).

Високочастотні паразитні коливання, промодульовані інформативним (небезпечним) сигналом за амплітудою, частотою і фазою (активна ПВЧГ) або за амплітудою і частотою (пасивна ПВЧГ), створюють канал витоку інформації.

ПВЧГ утворюється в елементах апаратури, які охоплені негативним зворотним зв`язком і не мають достатнього запасу стійкості, у кінцях ліній зв`язку між підсилювальними пристроями в моменти перемикань через виникнення перехідних процесів.

3.5 У процесі роботи ТЗПІ та ДТЗС можливий витік інформації через джерела електроживлення:

- у результаті проходження інформативного (небезпечного) сигналу через технічні засоби на вхідному опорі його джерела живлення може виникнути напруга, що несе сигнал, який містить інформативну складову. Через випрямний пристрій та силовий трансформатор цей сигнал поширюється мережевими лініями за межі контрольованої території;

- під час проходження мовного сигналу через кінцевий підсилювальний пристрій може мати місце нерівномірне споживання струму від джерела живлення. Струм, що споживається підсилювачем від мережі живлення, може бути промодульований інформативним (небезпечним) сигналом, який проходить через підсилювач.

3.6 Траси кабельних кіл, що несуть ІзОД, можуть прокладатися в одній кабельній каналізації з незахищеними каналами ТЗПІ та ДТЗС і проходити через спільні протяжні коробки і шафи.

Під час пересилання інформативного (небезпечного) сигналу одним колом у сусідніх колах - за їх паралельного пробігу - з`являються струми, наведені внаслідок електромагнітного впливу. Перехід електромагнітної енергії з одного кола в інше є можливим каналом витоку інформації.

Джерелами утворення інформативних (небезпечних) сигналів є ділянки, охоплені випадковими ємкісними і магнітними зв`язками. Такими ділянками можуть бути відрізки паралельного пробігу ліній, що несуть ІзОД, з незахищеними лініями, які уходять за межі контрольованої території, плінти кабельні, що служать для комутації вихідних ліній у кросах, монтажні колодки, роз`єми блоків, контакти перемикачів та реле, використовувані для комутації вихідних ліній, блоки, що зазнають впливу електромагнітного поля.

3.7 Витік інформації колом заземлення може статися з таких причин:

- за наявності контурів у системі заземлення, коли існують дві чи більше точки сполучення кіл, що несуть ІзОД, із заземлювачем;

- внаслідок недосконалості екранів і виникнення паразитних зв`язків. Витік може поширюватися як симетричними, так і несиметричними шляхами.

Джерелом утворення інформативних (небезпечних) сигналів є елементи кіл і схем, якщо ці елементи знаходяться під потенціалом таких сигналів і виходять з екранів.

3.8 Під час надходження високочастотних сигналів у нелінійні (або параметричні) кола, що несуть ІзОД, відбувається модуляція високочастотного сигналу. Таким чином, високочастотні коливання стають носіями інформативних (небезпечних) сигналів і створюють канал витоку інформації.

Лініями, на які подається або з яких знімається високочастотний сигнал, можуть бути незахищені лінії зв`язку, кола електроживлення, заземлення, керування і сигналізації, кола, утворені паразитними зв`язками, конструктивними елементами будинків, споруд, обладнання тощо. Джерелами інформативних (небезпечних) сигналів є нелінійні радіоелементи, на яких відбувається модуляція таких сигналів.

3.9 Під час виникнення несправностей в апаратурі або несанкціонованих діях обслуговуючого персоналу у схемах керування може виникнути небажана комутація інформативного (небезпечного) сигналу, яка призводить до виходу ІзОД у незахищений канал зв`язку.

Джерелами інформативного (небезпечного) сигналу цього каналу є пульти керування, щити розподілу та комутації, блоки контролю, реле, трансформатори, роз`єми, перемикачі або запам`ятовувальні пристрої, в яких може виникнути хибна комутація в результаті несправностей або несанкціонованих дій.

3.10 Основними параметрами можливого витоку інформації каналами ПЕМВН є:

- напруженість електричного поля інформативного (небезпечного) сигналу;

- напруженість магнітного поля інформативного (небезпечного) сигналу;

- величина звукового тиску;

- величина напруги інформативного (небезпечного) сигналу;

- величина напруги наведеного інформативного (небезпечного) сигналу;

- величина напруги шумів (завад);

- величина струму інформативного (небезпечного) сигналу;

- величина чутливості до впливу магнітних полів для точкового джерела;

- величина чутливості апаратури до впливу електричних полів (власна ємкість апаратури);

- величина чутливості до впливу акустичних полів;

- відношення "інформативний сигнал/шум";

- відношення напруги небезпечного сигналу до напруги шумів (завад) у діапазоні частот інформативного сигналу.

Зазначені параметри визначаються і розраховуються за результатами вимірювань у заданих точках.

Гранично допустимі значення основних параметрів є нормованими величинами і визначаються за відповідними методиками.

3.11 Відношення розрахункових (виміряних) значень основних параметрів до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації.

Методи захисту інформації від витоку по каналу побічних електромагнітних випромінювань та наведень (ПЕМВН) поділяють на ***пасивні*** та ***активні***. ***Пасивні методи захисту*** дозволяють зменшити рівень інформаційної цінності, або рівень випромінювання випромінюючого інформаційного сигналу ПЕМВН. ***Активні методи захисту*** полягають у створенні завад в каналах ПЕМВН, які ускладнюють приймання корисної інформації з перехоплених зловмисником сигналів.

***Пасивні методи захисту.***

Розрізняють три групи пасивних методів захисту:

● екранування;

● зменшення рівня випромінювань та наведень;

● зменшення рівня інформативної цінності сигналів.

2. Захист каналів зв’язку.

Захист інформації, що оброблюється ТЗПІ, здійснюється з використанням пасивних та активних методів та засобів.

Пасивні методи захисту направлені на:

- ослаблення інформаційних сигналів ТЗПІ на межі зони що контролюється до рівнів,

унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

- ослаблення наведень побічних електромагнітних випромінювань ТЗПІ на сторонні

провідники та з’єднувальні лінії ДТЗС, що виходять за межі зони що контролюється

до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

- виключення просочування інформаційних сигналів ТЗПІ до мереж

живлення що виходять за межі зони що контролюється до рівнів, унеможливлюючих

їх виділення засобами розвідки на шумовому фоні;

Активні методи захисту спрямовані на:

- створення просторових маскуючих електромагнітних завад з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

- створення маскуючих електромагнітних завад у сторонніх провідниках та з’єднувальних лініях ДТЗС з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

Ослаблення побічних електромагнітних випромінювань ТЗПІ та їх наведень у сторонні провідники здійснюється шляхом екранування та заземлення ТЗПІ та їх ліній заземлення.

Послаблення просочування інформаційних сигналів ТЗПІ до мереж електроживлення здійснюється шляхом фільтрації інформаційних сигналів.